IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR 1: **ACER Model: ES1-111** with serial number NXMSNAA0014391A6277600 black in color; 2: **SAMSUNG GALAXY SII IMEI**: 357930/04/079233-2; 3: **SAMSUNG GALAXY S4 IMEI** 990004373585128; 4: **MOTOROLA BLUR Hex MEID**: 0000002F39724-SJUG5230AA; 5: **SAMSUNG MODEL SGH-780 S/N**: D780GSMH; 6: **NOKIA Model-111 IMEI**: 358349051403730; 7: **IPHONE MODEL A1387 FCCID:** BCG-E2430Aand **TWITTER PROFILE WITH USERNAME:** @Hass2theJ (USER ID: 36548982) AT: https://twitter.com/hass2thej, THAT IS STORED AT PREMISES CONTROLLED BY TWITTER	Case No. 2:15mj248 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew W. Guinn, Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), Cincinnati Field Office ("CFO"), Columbus, Ohio, (hereinafter "your affiant") being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Section 2510 (7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to investigate and make arrests for offenses enumerated in Section 2516 of Title 18 , United States Code:

2. I make this affidavit in support of an application for a search warrant for information associated with a certain Twitter account that is stored at premises owned, maintained, controlled, or operated by Twitter, a social-networking company headquartered in San Francisco, CA. The information to be searched is described in the following paragraphs and in Attachment C. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b) (1)(A), and 2703(c)(1)(A) to require Twitter to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Twitter account:

3. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the Federal Bureau of Investigation (FBI) for over two years, since September 2012. Your affiant is currently assigned to the FBI Joint Terrorism Rask Force (hereinafter "JTTF") where he has been a Case Agent or Co-Case Agent for numerous International Terrorism investigations for the past two and a half years. During that time, your affiant has received specialized training in International Terrorism.

4. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other federal agencies, specifically the Federal Bureau of Investigation (FBI) and the Columbus, Ohio Police Department (CPD) and other law enforcement; from my discussions with witnesses involved in the investigation; and from my review of records and reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another law enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied on in reaching my conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

5. As will be detailed below (paragraphs 58 and 59), JEYLANI communicated with MOHAMUD via social media and via text messages. Given that the below listed devices either have the capability to send and receive either email, social media direct message communications, or text message communications, via cellular telephones that possess the capability to switch SIM cards between all of the cellular telephones, I allege the facts to show there is probable cause to believe that fruits and evidence of offenses involving violations of: (i) Title 18, United States Code §2339Aproviding material support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties and (v) Title 18, United States Code § 1001, false statements involving international or domestic terrorism.; may be found within the following devices:

- ACER Model: ES1-111; serial number NXMSNAA0014391A6277600 black in color;

- SAMSUNG GALAXY SII IMEI: 357930/04/079233-2;
- SAMSUNG GALAXY S4 IMEI: 990004373585128;
- MOTOROLA BLUR Hex MEID: 0000002F39724-SJUG5230AA;
- SAMSUNG MODEL SGH-780 S/N: D780GSMH;
- NOKIA Model-111 IMEI: 358349051403730;
- IPHONE MODEL A1387 FCCID: BCG-E2430A;

which are currently located in a secure FBI facility in Columbus, Ohio, as well as Twitter URL; https://twitter.com/hass2thej, which is stored at a premises controlled by Twitter.

6. Attachments A, B and C describe the devices to be searched and the Twitter Profile with user name to be searched. Attachments D, E and F describe the matters and things to be searched and seized within the devices and the Twitter Profile. All statements made in Attachments A, B, C, D, E and F are adopted into the body of this Affidavit as if fully set forth herein.

DEFINITIONS

The Role of the Computer

7. I know from my training and experience that computer hardware, software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of the crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, instrumentalities of crime and/or fruits of crime.

8. Based on my training and experience, I also know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard-drive and can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools.

When a person "deletes" a file on a home computer, the data contained in the files does not actually disappear; rather the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is space on the hard drive that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

9. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache". The browser typically maintains fixed amounts of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

IP Addresses

10. An Internet Protocol ("IP") address is a unique numeric identifier assigned to every computer attached to the Internet. An Internet service provider (ISP) normally controls a range of several hundred (or even thousands of) IP addresses, which it assigns to its customers for their use.

11. IP addresses are conventionally written in the dot-punctuated form num1.num2.num3.num4 (e.g., 216.109.118.74). There are two types of IP addresses— static and dynamic. A static IP address is one that is permanently assigned to a given computer on a network. With dynamic IP addressing, however, each time a computer establishes an Internet connection, that computer is assigned a different IP address. For example, each time a customer with a dynamic IP address establishes an Internet connection; he or she is randomly assigned an IP address from the block of IP addresses controlled by their Internet Service Provider. When the customer ends the session, the temporarily assigned IP address is placed back into the pool of IP addresses available for temporary assignment to other subscribers. Customers using broadband Internet services are typically assigned IP addresses that are technically dynamic, but which may remain unchanged for longer, but not indefinite, periods of time (e.g., one week). It is possible

to associate a particular user account with a particular dynamic IP address at a specific date and time. The government may then, through the use of appropriate legal process, compel the ISP associated with that IP address to reveal information concerning the physical location of the computer assigned the IP address at that specific date and time as well as the identity of the subscriber associated with that account.

THE ROLE OF THE CELLULAR TELEPHONE

12. The following have indicated meaning in this affidavit: A cellular telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through wireless networks of transmitters /receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the telephone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing play back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Wireless telephones may also include global positioning system technology for determining the location of the device.

ELECTRONIC DEVICES AND STORAGE

13. Bases on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information for long periods of time, it can sometimes be recovered with forensic tools.

14. As described above and in Attachment A and B, this application seeks permission to search the following devices:

- ACER Model: ES1-111; serial number NXMSNAA0014391A6277600 black in color;
- SAMSUNG GALAXY SII IMEI: 357930/04/079233-2;
- SAMSUNG GALAXY S4 IMEI: 990004373585128;

- MOTOROLA BLUR Hex MEID: 0000002F39724-SJUG5230AA;
- SAMSUNG MODEL SGH-780 S/N: D780GSMH;
- NOKIA Model-111 IMEI: 358349051403730;
- IPHONE MODEL A1387 FCCID: BCG-E2430A.

15. Searching for the evidence described in Attachment D and E may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment D and E, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the FBI and its agents intend to use whatever data analysis techniques appear necessary to locate and retrieve evidence described in Attachment B.

TWITTER DESCRIPTION

16. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at http://www.twitter.com. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

17. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

18. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

19. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

20. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

21. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (i.e., a list of all "mentions" and "replies" for that username).

22. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

23. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location"

function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

24. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with http://t.co. This link service measures how many times a link has been clicked.

25. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's "followers" list) and a list of people whom that user follows (i.e., the user's "following" list). Twitters users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

26. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

27. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

28. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

29. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

30. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

31. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

32. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, communications, "tweets" (status updates) and "tweeted" photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses; investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter

builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculpate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

OVERVIEW OF THE INVESTIGATION

34. On June 24, 2014, the FBI opened an investigation into Abdirahman Sheik MOHAMUD (Date of Birth: September 1, 1991, hereinafter MOHAMUD) who is a Columbus, Ohio resident and a Naturalized United States Citizen.

35. MOHAMUD departed the United States on April 18, 2014 for the purpose of fighting in Syria and to provide material support for al-Nusrah Front ("al-Nusrah"), an organization affiliated with al-Qa'ida that is designated by the U.S. Secretary of State as a foreign terrorist organization (FTO). MOHAMUD's brother, Abdifatah ADEN, was in Syria at that time fighting with al-Nusrah and Ahrar al-Sham, a group linked to al-Nusrah also fighting in Syria.

36. While in Syria, MOHAMUD trained with al-Nusrah on use of weapons and tactics and then was instructed by al-Nusrah to return to the U.S. and commit an act of terrorism on behalf of al-Nusrah. MOHAMUD returned to the U.S. on June 8, 2014, and while in the United States, your Affiant believes MOHAMUD conspired with others, including Hassan Sheikh JEYLANI, to plot the kidnapping and murder of United States-based soldiers.

PROBABLE CAUSE

a) 18 U.S.C. §§ 2339A, 2339B, 1117, and 1114

37. The FBI has been investigating JEYLANI, and other individuals believed to be part of MOHAMUD's core group of friends and associates, since on or about September 2014, as potential co-conspirators in MOHAMUD's plot to carry out a terrorist attack in the United States.

UNNAMED PERSON #4

38. Recently, under the advice of his attorney, Unnamed Person #4 provided a statement against his own interests regarding the roles in the aforementioned plot involving MOHAMUD, Hassan JEYLANI (hereinafter JEYLANI), Jibril ALI (hereinafter ALI), Abdiqani ADEN (hereinafter ADEN), Faisal ADEN (hereinafter FAISAL), and Abullahi AHMED (hereinafter AHMED.) Unnamed person #4 is described as an active participant in this plot.

39. Unnamed Person #4 was radicalized by Jabhat al-Nusrah and given direction to do harm in the United State. Unnamed Person #4 was told to save Aafia SIDDIQUI by grabbing and kidnapping American soldiers and taking them as hostages. After returning to the United States, Unnamed person #4 told JEYLANI, ALI, ADEN, FAISAL, and AHMED about the plot, and all agreed to participate. They would bring up new ideas in furtherance of the plan. All agreed to raise money for the plan, specifically JEYLANI. The plan was to go down to Texas where SIDDIQUI was located, grab civilians or soldiers, and try to negotiate for her release. Unnamed Person #4 purchased a plane ticket to Texas which he stated was for reconnaissance in furtherance of the plan. The group talked about how this would work and about getting guns and who to get guns from. They talked about clothing which was going to be military clothing to

make people think they were Jabhat al-Nusrah. They would wear ski masks to cover their faces and have handguns. The group discussed doing reconnaissance on military installations. Unnamed Person #4, AHMED, and ADEN did reconnaissance on a military installation in Columbus. Even after the group members knew they were being followed by the law enforcement (FBI), they all continued to meet and cultivate their plans.

UNNAMED PERSON #1

40. On February 18, 2015 and February 19, 2015, the FBI interviewed Unnamed Person #1. Unnamed Person #1 is described as a peer and associate of MOHAMUD's. Your Affiant believes the following exchanges indicate that MOHAMUD was in the country of Syria in April to May of 2014, and received training and instruction from a high ranking jihadist to return to the United States and do something there, which caused MOHAMUD to develop the plan to recruit a trusted core group of individuals and conduct an attack in the United States against military targets. As further explained below, MOHAMUD indicated that he knows some people on the west side of Columbus, and they are going to get together and go somewhere to kill troops.

41. During the interview, Unnamed Person #1 described statements MOHAMUD made to Unnamed Person #1 after MOHAMUD returned from overseas. While he (MOHAMUD) was in Syria, he talked with a high ranking jihadist who told him you have an American passport, you have lived in America for nineteen years, go back and do something there (in the United Sates). This high ranking leader in Syria gave him (MOHAMUD) the task to go kill groups in uniform, who work for the U.S. Government on an army base. MOHAMUD stated that is why he returned to the U.S. and that his plan was to lay low and get with a group of "guys." MOHAMUD told Unnamed Person #1 that he knows some people on the west side of Columbus and that they are going to get together and go somewhere to kill troops. Prior to this direction, MOHAMUD had received training in Syria on how to fire guns, clean guns, fix weapons jams, hand to hand combat, knives, tactics and explosives. They would do different types of drills, including training on how to go into a house, kill the people inside and take what they could get.

42. Unnamed Person #1 was shown Ohio DMV photos of several individuals who FBI believes are MOHAMUD's co-conspirators, and identified several of them as being members of MOHAMUD's core group of friends. Specifically, Unnamed Person #1 identified the individuals in the photos as "WAACE" (true name Abdiqani ADEN), "FAZE" (true name Faisel Osman ADEN), and "Jibril" (true name Jibril ALI). Unnamed Person #1 also recognized a photo of Abdullahi Dahir AHMED, but did not know AHMED's name. Unnamed Person #1 identified all four of these individuals as the group that is always with MOHAMUD. The group usually plays basketball at the Grove City "Y" on Mondays and Wednesdays from 7 to 10 pm.

UNNAMED PERSON #2

43. On March 2, 2015, the FBI interviewed Unnamed Person #2. Unnamed Person #2 is described as a peer and associate of MOHAMUD's. Your affiant believes the following exchanges corroborate Unnamed Person #1's statements; that MOHAMUD was in the country of Syria, and received instruction and training to return to the United States to organize an attack.

44. A couple of weeks after MOHAMUD returned from his overseas trip, he and Unnamed Person #2 were hanging out at MOHAMUD's house. MOHAMUD went on to tell Unnamed Person #2 that he went to SYRIA where he went to a training camp where he did a lot of exercises and got fit. There were other groups of people at the camp training. MOHAMUD stated he switched posts, got supplies, and at least once said he had the night post. MOHAMUD tried to meet up with his brother (Abdifitah ADEN) while in Syria but was unable to because they were at different locations. MOHAMUD mentioned the names of groups that he was with but Unnamed Person #2 could not recall the names. The only name he could recall was, "DOLUTA ISLAMIA" but Unnamed Person #2 was not familiar with that name and did not know if it meant anything.

45. Unnamed Person #2 stated that MOHAMUD told him that he was involved in one small firefight and a couple of close calls. MOHAMUD never mentioned that he killed anyone. During the same conversation, MOHAMUD mentioned that he had an AK-47 while in Syria.

While MOHAMUD was overseas, he sent Unnamed Person #2 a SNAPCHAT[1] video. The video was of MOHAMUD, walking around with an AK-47 slung over his shoulder. MOHAMUD was wearing a green Pakistani style robe and a white and black turban. In the video, MOHAMUD said something like, "got my AK, doing my training."

46. Also during this conversation, MOHAMUD expressed his opinions of the U.S. (United States) to Unnamed Person #2. MOHAMUD said this country (United States) is corrupt, Guantanamo is a huge problem and MOHAMUD wanted to fix it; MOHAMUD wanted to do something "big", like go to TEXAS, capture three to four soldiers and kill them, execution style. MOHAMUD wanted to get more people to help him and Unnamed Person #2 was sure MOHAMUD was trying to recruit him. He tried to recruit Unnamed Person #2 by asking him a lot of questions about his life, such as, what are you doing now, school is a waste of time, and there are more important things. All of the questions implied that Unnamed Person #2 should help MOHAMUD.

47. When asked by Interviewing Agents if anyone else knew about MOHAMUD's activities or plans to carry out a domestic attack, Unnamed Person #2 replied that WAACE (ADEN) and JIBRIL (ALI) most likely do. They share similar opinions as MOHAMUD and know MOHAMUD's opinions very well. They dislike America but not to the same level as MOHAMUD. WAACE (ADEN) and JIBRIL (ALI) used to be really bad kids when they were younger but as they grew up they became more religious.

48. According to Unnamed Person #2, several kids used to play basketball with MOHAMUD but the core group was "The RIVERPOINTE kids." They included LE'BELL (Abdullahi AHMED), JIBRIL (ALI), WAACE (ADEN) or ABDIQANI, and another named person Unnamed Person #2 saw the guys with MOHAMUD a lot. Someone always had a car to drive them to the various locations.

49. When Interviewing Agents asked Unnamed Person #2 why MOHAMUD chose TEXAS for an attack, Unnamed Person #2 replied that MOHAMUD picked TEXAS because he

[1] Snapchat is a photo messaging application. Using the application, users can take photos, record videos, add text and drawings, and send them to a controlled list of recipients. These sent photographs and videos are known as "Snaps". Users set a time limit for how long recipients can view their Snaps, the range is from 1 to 10 seconds, after which they will be hidden from the recipient's device and deleted from Snapchat's servers.

had family or some close friends in TEXAS so he had a place to stay and he could tell his mother he was just going to visit them.

MOHAMUD FLIGHT RESERVATION TEXAS

50. On November 19, 2014, the FBI was notified that MOHAMUD was scheduled to travel on American Airlines flight 2310 departing Columbus, Ohio for Dallas, Texas. However, to your Affiant's knowledge, MOHAMUD never boarded that flight.

L.E.P.D. FIREARMS RANGE

51. In connection with this matter, the FBI has also interviewed Unnamed Person #3, who is described as an employee of L.E.P.D. Firearms and Range. Unnamed person #3 provided information derived from other employees of L.E.P.D. Firearms and Range, as well as recorded video surveillance observations. Your Affiant believes the following interview represents an action taken by MOHAMUD to provide training to individuals who included members of MOHAMUD's core group of friends, as identifies by Unnamed Persons #1 and #2.

52. Unnamed Person #3 reported that on September 5, 2014, MOHAMUD and three other individuals parked their black four-door Honda bearing Ohio License Plate EUG8416, and exited the vehicle. The four males entered the store (L.E.P.D. Firearms and Range) and looked at pistols in front of the store. The group then rented a FNS 9mm pistol, purchased a box of ammunition, targets and thirty minutes of range time. Three of the males provided their identification and were identified as MOHAMUD, Faisal Osman ADEN (hereinafter FAISAL) and Hassan Sheikh JEYLANI (JEYLANI). The fourth male was under the age of twenty one; however, a February 24, 2015 interview of JEYLANI revealed that Abdullahi Dahir AHMED (hereinafter AHMED) was the fourth male, who was under the age of twenty-one and who accompanied MOHAMUD, JEYLANI and FAISAL to the range.

MOHAMUD ARRESTED

53. On February 25, 2015, MOHAMUD was arraigned in Franklin County Common Pleas Court on State of Ohio charges of Soliciting or Providing Support for an Act of Terrorism

(2909.22) (F-3) and Money Laundering in Support of Terrorism (2909.29) (F-5). On February 24, 2015, JEYLANI was interviewed by FBI agents (further details of this interview are provided below).

JEYLANI

54. On March 2, 2015, approximately one week after MOHAMUD's arrest and JEYLANI's interview, FBI agents were notified that Hassan JEYLANI had booked a flight itinerary for March 4, 2014 on board United Airlines (UA) flight 5898, departing Columbus, Ohio (CMH) for Newark, NJ. JEYLANI was scheduled to continue aboard Scandinavian (SK) flight 904, departing Newark, NJ for Stockholm, Sweden.

55. On March 4, 2015, a supervisor (hereinafter "Unnamed Person #5) for United Airlines (UA) was interviewed at Port Columbus International Airport. Unnamed Person #5 attempted to check United Airlines passenger Hassan Sheikh JEYLANI onto flight UA 5898. JEYLANI used his United States Passport as identification. Unnamed Person #5 informed JEYLANI that he was not allowed to fly. Also present at the UA ticket counter were ADEN and AHMED. Police then intervened and escorted JEYLANI, ADEN and AHMED from the counter.

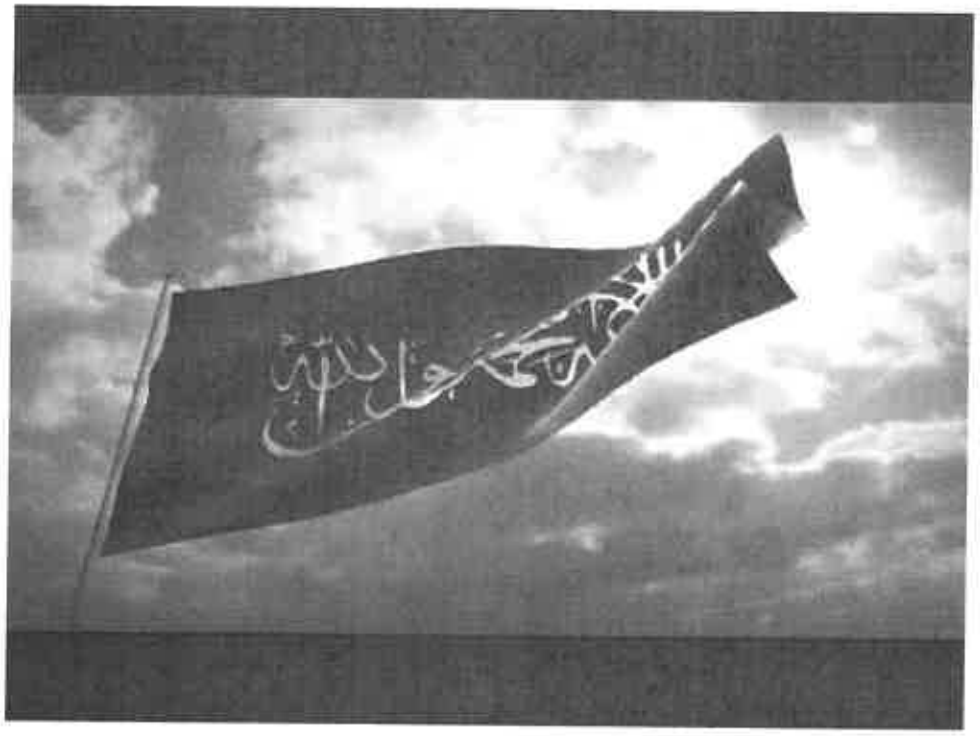
b. 18 U.S.C. §1001

56. On February 24, 2015, JEYLANI was interviewed by FBI agents. JEYLANI was informed by interviewing agents that lying to a federal officer is a crime under Title 18 United States Code § 1001, and JEYLANI confirmed to the interviewing agents that he understood this section of United States Code as it was explained to him. Agents informed JEYLANI that they were interested in MOHAMUD and the circumstances surrounding the death of MOHAMUD's brother Abdifitah ADEN.

57. JEYLANI said that he knew MOHAMUD from the mosque, but did not socialize with him in any way. JEYLANI stated that he did not know how to get in contact with MOHAMUD, and that he had never called or texted him from his phone number, 614-377-3125, nor any other number.

58. On March 6, 2015, FBI analysts, reviewing information collected from MOHAMUD's Samsung Galaxy S III phone, discovered eleven incoming text messages from JEYLANI to MOHAMUD (dated: September 8, 2014) from JEYLANI's cellular telephone, 614-377-3125, to MOHAMUD's Google Voice number. In the text messages, JEYLANI addressed MOHAMUD as "Akhi,"[2] and asked MOHAMUD to try to get back to the job that "Abdul" (presumed ADEN) and "gibril" (presumed ALI) were at, that they needed "quick money," and that MOHAMUD needed to call an individual to let her know that they were "coming back."

59. A review of JEYLANI's publicly available Twitter Page, https://twitter.com/hass2thej (ID: 36548982), revealed that JEYLANI, ADEN and FAISAL were all following one another on Twitter. Although not extreme in and of itself, JEYLANI has approximately seventy-three tweets which primarily focused on many offenses in the Koran that makes one a "Kufaar," or a "disbeliever," as described by JEYLANI. Also, of noted significance is the following black flag image identified on JEYLANI's Twitter page:



60. The Black Flag is a symbol with the Islamic Shahada [Islamic confession translated in English as "There is no god but God, Muhammad is the messenger of God"] in

[2] "Akhi" is a common Arabic term many use in greeting one-another which translates to "my brother."

white Arabic script on a solid black background. It is believed in Islam to originally be one of the flags flown by the Prophet Muhammad. However, it has become used in the last two decades as a flag used by al-Qa'ida and other terrorist organizations to symbolize offensive war for the establishment of the Caliphate. Al-Nusrah is an al-Qa'ida affiliate.

DEVICES TO BE SEARCHED PHONES/COMPUTER

61. On March 9, 2015, JEYLANI was arrested by the Columbus Police Department and charged with aggravated robbery (Code 2911.01) (F-1.) Pursuant to the aggravated robbery charges, JEYLANI's residence was searched and the following electronic devices seized:

- ACER Model: ES1-111; serial number NXMSNAA0014391A6277600 black in color;
- SAMSUNG GALAXY SII IMEI: 357930/04/079233-2;
- SAMSUNG GALAXY S4 IMEI: 990004373585128;
- MOTOROLA BLUR Hex MEID: 0000002F39724-SJUG5230AA;
- SAMSUNG MODEL SGH-780 S/N: D780GSMH;
- NOKIA Model-111 IMEI: 358349051403730;
- IPHONE MODEL A1387 FCCID: BCG-E2430A.

62. Also seized pursuant to the Columbus Police Department, were multiple United States Passports, three envelopes containing a total of approximately $2900 in cash and multiple credit cards

63. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

b. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

64. In light of these concerns, I hereby request the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

65. By this affidavit and application, I request that the Court issue a search warrant allowing agents to search for the items described in "Attachment A, B, and C." The information sought in the accompanying Application is relevant to an on-going investigation and premature disclosure of this Application and related documents may adversely impact the investigation. Therefore, it is requested that this Application and the related documents be filed under seal.

CONCLUSION

66. Based on these facts, there is probable cause to believe that there are fruits and evidence, as further described in Attachments D, E and F, of: (i) Title 18, United States Code §2339A, providing material support to terrorists, (ii) Title 18, United States Code §2339B, providing material support to a designated foreign terrorist organization; (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate, (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties and (v) Title 18, United States Code § 1001, false statements involving international or domestic terrorism.; may be found within the following devices:

- ACER Model: ES1-111; serial number NXMSNAA0014391A6277600 black in color;
- SAMSUNG GALAXY SII IMEI: 357930/04/079233-2;
- SAMSUNG GALAXY S4 IMEI: 990004373585128;
- MOTOROLA BLUR Hex MEID: 0000002F39724-SJUG5230AA;
- SAMSUNG MODEL SGH-780 S/N: D780GSMH;
- NOKIA Model-111 IMEI: 358349051403730;
- IPHONE MODEL A1387 FCCID: BCG-E2430A,

as well as Twitter PROFILE with USERNAME: @Hass2theJ (USER ID: 36548982). Specifically, in this case the cell phone may contain evidence of JEYLANI's phone calls and text messages with MOHAMUD which relates to the planning and execution of the plot in coordination with terrorism suspect MOHAMUD to conspire with others the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties, and that this device may also contain contact information for other individuals who also participated in the plot with MOHAMUD.

Respectfully submitted,

Matthew W. Guinn

Special Agent

Federal Bureau of Investigation

Subscribed and sworn to before me on March 17, 2015

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

ACER Model: ES1-111with NXMSNAA0014391A6277600 that is currently located at a secure FBI facility in Columbus, Ohio. The computer is black in color.

ATTACHMENT B

DESCRIPTION OF PROPERTY TO BE SEARCHED

The items to be searched are currently located at a secure FBI facility in Columbus, Ohio. The cellular telephones to be searched are described as follows:

- SAMSUNG GALAXY SII IMEI: 357930/04/079233-2;
- SAMSUNG GALAXY S4 IMEI: 990004373585128;
- MOTOROLA BLUR Hex MEID: 0000002F39724-SJUG5230AA;
- SAMSUNG MODEL SGH-780 S/N: D780GSMH;
- NOKIA Model-111 IMEI: 358349051403730;
- IPHONE MODEL A1387 FCCID: BCG-E2430A.

ATTACHMENT C

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Twitter profile with username @Hass2theJ (USER ID: 36548982) at https://twitter.com/hass2thej that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.

ATTACHMENT D

ITEMS TO BE SEIZED

1. All records relating in any manner, directly or indirectly, to violations of United States Code(s) noted in the Affidavit, including correspondence concerning these crimes (whether in hard copies or electronic form), personal information concerning victims of these crimes, electronic correspondence and records identifying co-conspirators of these crimes.

   a. The terms "records" and "information" includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including but not limited to floppy diskettes, hard disks, zip disks, CD-ROMS, thumb drives, optical discs, backup tapes, printer buffers, smart cards, pagers, personal digital assistants, as well as printouts or readouts from any magnetic storage device);

2. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

3. Any bank account numbers stored on any storage devices in the computer.

4. Any user attribution data stored on any storage devices in the computer.

5. Any personally identifiable information stored on any storage devices in the computer, such as, but not limited to, social security numbers, dates of birth, full names, addresses, and telephone numbers.

6. Any data on the computer showing the addition or removal of any storage devices.

ATTACHMENT E

ITEMS TO BE SEIZED

The electronically stored contents, including, but not limited to evidence of ownership, subscribers, address books, call logs, phone books, photographs, voice mail, messages, text messages, images and video and any other stored electronic data, and records and information relating to cellular telephones including records relating to incoming and outgoing calls, and recorded phone history for the following devices:

- SAMSUNG GALAXY SII IMEI: 357930/04/079233-2;
- SAMSUNG GALAXY S4 IMEI: 990004373585128;
- MOTOROLA BLUR Hex MEID: 0000002F39724-SJUG5230AA;
- SAMSUNG MODEL SGH-780 S/N: D780GSMH;
- NOKIA Model-111 IMEI: 358349051403730;
- IPHONE MODEL A1387 FCCID: BCG-E2430A.

ATTACHMENT F

ITEMS TO BE SEIZED

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment C is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment C:

a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

b. All past and current usernames, account passwords, and names associated with the account;

c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

d. All IP logs and other documents showing the IP address, date, and time of each login to the account;

e. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

f. All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;

g. All information from the "Connect" tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a

list of all Tweets that include the username associated with the account (i.e., "mentions" or "replies");

h. All photographs and images in the user gallery for the account;

i. All location data associated with the account, including all information collected by the "Tweet With Location" service;

j. All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

k. All data and information that has been deleted by the user;

l. A list of all of the people that the user follows on Twitter and all people who are following the user (i.e., the user's "following" list and "followers" list);

m. A list of all users that the account has "unfollowed" or blocked;

n. All "lists" created by the account;

o. All information on the "Who to Follow" list for the account;

p. All privacy and account settings;

q. All records of Twitter searches performed by the account, including all past searches saved by the account;

r. All information about connections between the account and third-party websites and applications;

s. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of (i) Title 18, United States Code §2339A, providing material support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties and (v) Title 18, United States Code § 1001involving JEYLANI since April 2014 including, for each user ID identified on Attachment C, information pertaining to the following matters:

a. Based on the foregoing , your affiant believes that JEYLANI was an active participant in conspiring with MOHAMUD, FAISAL, ADEN, ALI and AHMED to violate the aforementioned statutes, and that JEYLANI communicated with MOHAMUD via his Twitter URL based on your affiant's knowledge that MOHAMUD, ADEN and FAISAL were Twitter followers of JEYLANI's.

b. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Twitter account owner;

c. Evidence indicating the Twitter account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).